국내 유명 웹하드를 통해 유포되는 njRAT 악성코드

By ATCP

Published: 2020-08-19 · Archived: 2026-04-06 01:31:44 UTC

njRAT 악성코드는 사용자의 개인 정보를 탈취하며 공격자의 명령을 받아 실행할 수 있는 RAT 악성코드로, 국내에서 개인을 상대로 꾸준히 유포되고 있다.

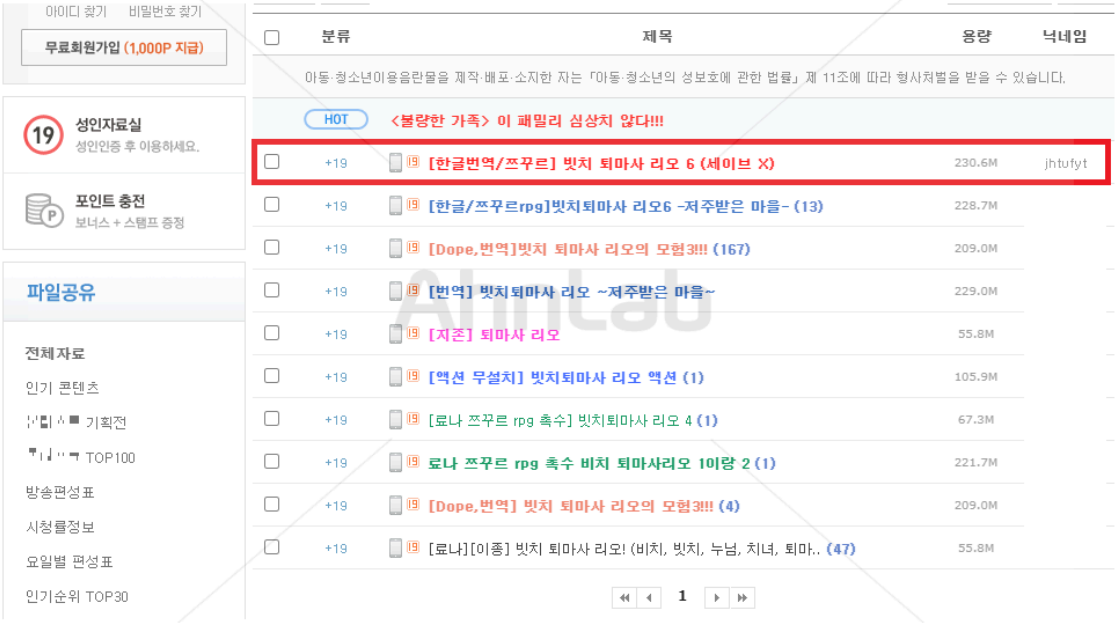
ASEC 주간 악성코드 통계 (20200803 ~ 20200809)

ASEC 분석팀에서는 ASEC 자동 분석 시스템 RAPIT를 활용하여 알려진 악성코드들에 대한 분류 및 대응을 진행하고 있다. 여기에서는 2020년 8월 3일 월요일부터 2020년 8월 9일 일요일까지 수집된 한 주간의 통계를..

https://asec.ahnlab.com/1367

진단 로그를 분석한 결과 njRAT은 주로 웹하드나 토렌트 등 자료 공유 사이트를 통하여 게임, 인증 툴, 유틸리티 등의 정상 파일로 위장하여 유포되며, 대부분의 경우 원본 프로그램이 실행됨과 동시에 악성코드가 감염되어 사용자 입장에서는 감염 사실을 파악하기 쉽지 않다.

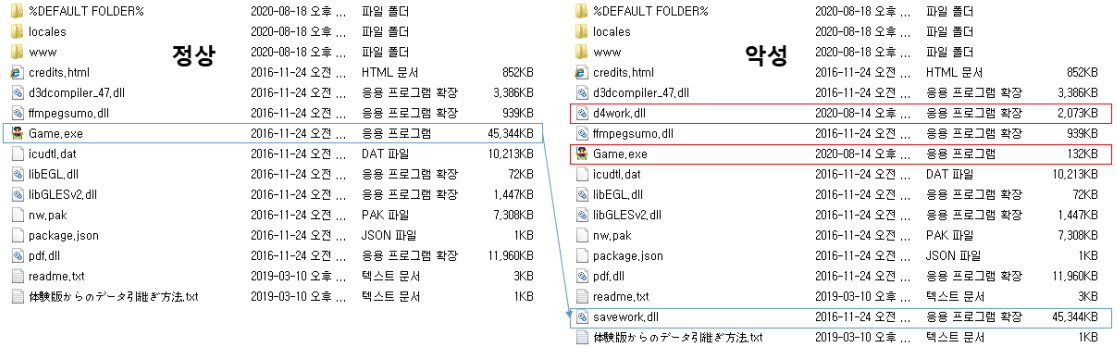
ASEC 분석팀은 njRAT 악성코드가 국내 웹하드 사이트를 통해 유포 중인 사례를 소개하고자 한다. 최근 유포된 njRAT의 파일명을 기반으로 역추적한 결과 다음과 같이 국내 유명 웹하드 사이트에서 유포 중인 게시글을 확인할 수 있었다.



[그림1] 웹하드 게시판에 업로드된 악성코드

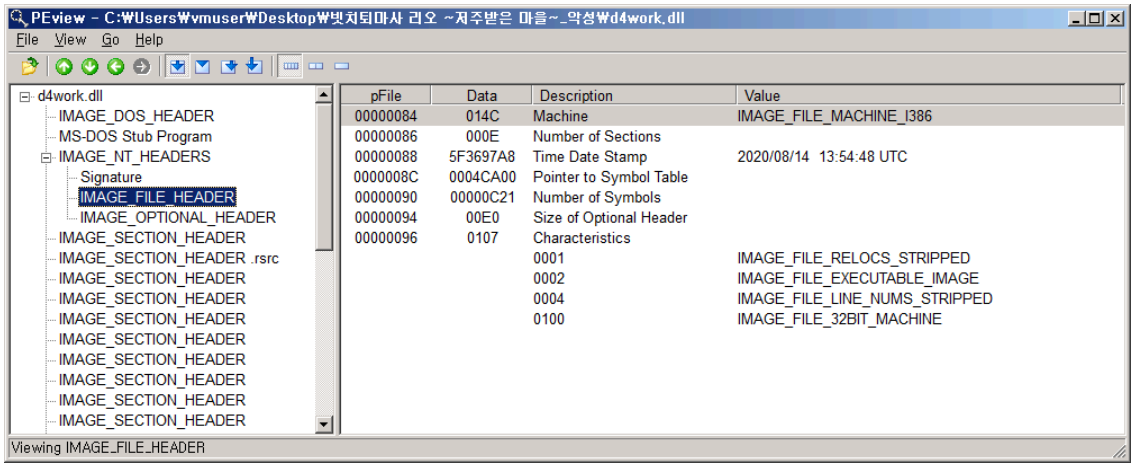
[그림2] 악성코드 포함된 압축파일

또한 동일 사이트에서 이전에 업로드된 악성코드가 포함되지 않은 원본 자료를 찾을 수 있었으며 두 자료를 비교해본 결과 다음과 같은 차이점이 있었다.



[그림3] 정상파일과 악성파일 비교

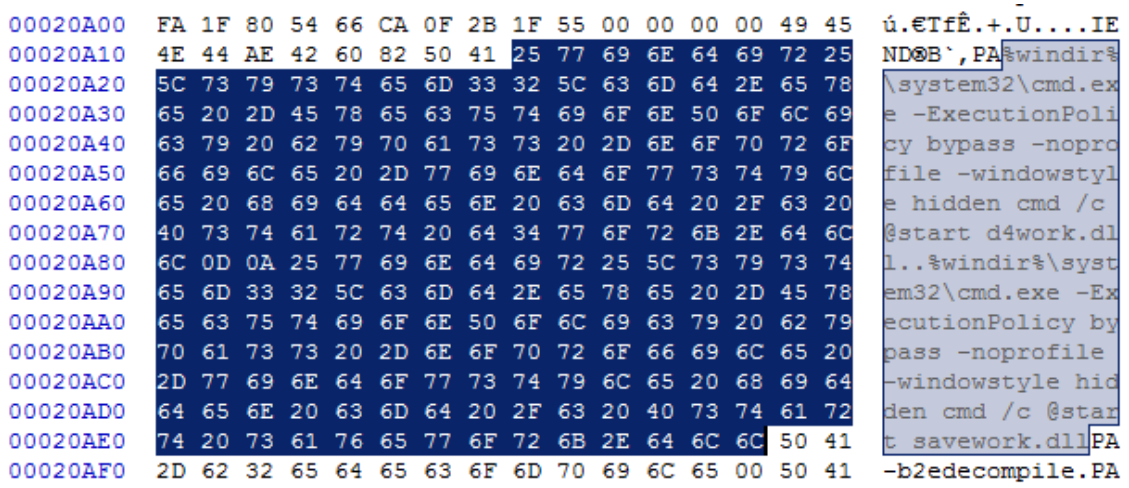
악성 압축파일 내부에는 정상과 다르게 savework.dll과 d4work.dll 파일이 추가되었다. savework.dll은 이름이 변경된 정상 Game.exe 파일이며, d4work.dll은 njRAT 악성코드이다. 두 파일 모두 파일 확장명은 .dll 이지만 실제로는 실행파일(.exe)이다.



[그림4] d4work.dll의 PE 정보

공격자는 원본 자료에서 게임 실행 파일의 이름을 변경하고 악성코드를 추가한 뒤 악성코드와 게임을 동시에 실행하는 실행파일을 제작하여 유포하였다.

공격자가 제작하여 추가한 Game.exe는 Vbs2Exe로 제작된 파일이며 정상 Game.exe 아이콘으로 위장하였다. Vbs2Exe는 스크립트 언어인 VBS를 PE 형태의 실행파일로 만들어 주는 프로그램으로, 이로 빌드된 파일은 리소스 영역의 명령어를 로드하여 실행 되는 구조를 갖는다.



[그림5] 악성 Game.exe의 리소스 영역

해당 파일이 실행되면 다음 명령어를 통해 d4work.dll(njRAT 악성코드)와 savework.dll(원본 Game.exe)가 실행되어 악성코드에 감염되며 게임이 실행된다.

- %windir%system32cmd.exe -ExecutionPolicy bypass -noprofile -windowstyle hidden cmd /c @start d4work.dll
- %windir%system32cmd.exe -ExecutionPolicy bypass -noprofile -windowstyle hidden cmd /c @start savework.dll

d4work.dll 파일 실행 시 %appdata% 하위에 특정 파일명으로 자가복제 후 바로가기를 생성하여 레지스트리를 통해 자동실행 등록한다. 이후 C2에 접속하여 공격자의 명령을 대기하며, 공격자의 명령에 따라 다양한 악성 행위를 수행 가능하다.

최근 약 일주일간 유포된 njRAT 악성코드 중 웹하드를 통해 유포된 것으로 추정되는 사례의 파일명 및 상대경로명 일부는 다음과 같다. 대다수가 게임 및 유틸리티를 위장하여 유포되고 있으며, 특정 웹하드가 아닌 다수의 국내 웹하드 사이트가 유포지가 되고 있는 것을 확인할 수 있다.

- X디스크[rj289299]asylum세라앤노엘 -붙잡힌 공주의 행방-**game.exe**
- 프린세스퀘스트 수치와굴욕 ver101새 폴더**game.exe**
- motherslessons**game.exe**
- 핫한 여자랑 노는게임!the lady is in heat**d3dcompiler_46.dll**
- fileXX(190329)有料プラン限定rpg　bewitching sword2 ver.1.0**steam.com**
- 윈도우 10 정품 인증기**윈도우10 정품 인증기.exe**
- 복음의 apostle**d4work.dll**
- X디스크sinnenn_ver1game**d4work.dll**
- 하드번호 변경하기**set up.exe**
- 한컴2020**set up.exe**
- 서든핵sa (1)**sa.exe**
- X디스크대출아내psaa**reget.exe**
- 무인도생활**d3dcompiler_46.dll**
- 나루토**reget.exe**

- 파일X 다운로드[rj291663] 여기사 프레이 1.0**reget.exe**

이와같이 국내 웹하드 등 자료공유 사이트를 통해 악성코드가 활발하게 유포되고 있어 주의가 필요하다. 자료 공유 사이트에서 다운받은 실행파일은 각별히 주의해야 하며, 유틸리티 및 게임 등의 프로그램은 반드시 공식 홈페이지에서 다운로드하는 것을 권장한다.

[V3 진단]

- Trojan/Win32.Loader.C4183142
- Backdoor/Win32.Korat.C4182520

MD5

1c359f9edf43f2986f782b631f418ebb

88e4da56049f4aa60a1ebeb47ad4dafa

추가 IoC는 ATIP에서 제공됩니다.

URL

http[:]//so69[.]kro[.]kr/

추가 IoC는 ATIP에서 제공됩니다.
